THE DISTRIBUTION OF CLASS NUMBERS OF PURE NUMBER FIELDS (Diophantine Problems and Analytic Number Theory)

数理解析研究所講究録 1319 巻 2003 年 193-197

THE DISTRIBUTION OF CLASS NUMBERS OF PURE NUMBER FIELDS

MANFRED PETER

Much is known about the statistical distribution of class numbers of binary quadratic forms and quadratic fields. Let $d \equiv 0, 1 \bmod 4$ and d not a perfect square. Define $h(d)$ as the number of equivalence classes of primitive binary quadratic forms with discriminant d (and positive definite in case $d < 0$). For $d > 0$, let $\epsilon_d := (u_d + v_d\sqrt{d})/2$, where (u_d, v_d) is the fundamental solution of Pell's equation $u^2 - dv^2 = 4$. If d is a fundamental discriminant then $h(d)$ is also the class number of $\mathbb{Q}(\sqrt{d})$ in the narrow sense.

Gauß [5] conjectured and Mertens [9] and Siegel [11] later proved that

$$\sum_{0<d\leq x} h(d) \log \epsilon_d \sim \frac{\pi^2}{18\zeta(3)} x^{3/2}, \quad \sum_{0>d\geq -x} h(d) \sim \frac{\pi}{18\zeta(3)} x^{3/2}.$$

Chowla and Erdös [3] proved that there is a continuous distribution function F such that for all $z \in \mathbb{R}$,

$$\lim_{x\to\infty} \frac{1}{x/2} \#\left\{0 < d \leq x \,\middle|\, \frac{h(d)\log \epsilon_d}{d^{1/2}} \leq e^z\right\} = F(z),$$

$$\lim_{x\to\infty} \frac{1}{x/2} \#\left\{0 > d \geq -x \,\middle|\, \frac{h(d)\pi}{|d|^{1/2}} \leq e^z\right\} = F(z).$$

Elliott [4] showed that $F \in C^\infty(\mathbb{R})$ and it has the characteristic function

$$\Psi(t) = \prod_p \left(\frac{1}{p} + \frac{1}{2}\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p}\right)^{-it} + \frac{1}{2}\left(1 - \frac{1}{p}\right)\left(1 + \frac{1}{p}\right)^{-it}\right), \quad t \in \mathbb{R}.$$

Barban [1] proved that for $q \in \mathbb{N}$, the $q-th$ moment β_q of $F(\log z)$ exists and that

$$\lim_{x\to\infty} \frac{1}{x/2} \sum_{0<d\leq x} \left(\frac{h(d)\log \epsilon_d}{d^{1/2}}\right)^q = \beta_q = \sum_{n\geq 1} \frac{\varphi(n) d_q(n^2)}{2n^3},$$

$$\lim_{x\to\infty} \frac{1}{x/2} \sum_{0>d\geq -x} \left(\frac{h(d)\pi}{|d|^{1/2}}\right)^q = \beta_q,$$

where φ is Euler's totient function and $d_q(n)$ is the number of ways one can write n as a product of q positive integers. For all these results, error term estimates can be given (see [2], [6], [10], [12], [13]).

It seems that for number fields of higher degree, no analoguous results are known. The Brauer-Siegel Theorem (see, e.g., [8], Chapter XVI) gives a rough idea of the size of the class number times the regulator: Let k range over a sequence of number fields which are galois over $\mathbb{Q}$ such that $n/\log d \to 0$, where $n := [k : \mathbb{Q}]$ is the degree and $d = d_{k/\mathbb{Q}}$ is the absolute discriminant of k. Let h_k be the class number of k and R_k its regulator. Then

$$\frac{\log(h_k R_k)}{\log d^{1/2}} \to 1.$$

When looking for more precise information on the value distribution of

$$\frac{h_k R_k}{d^{1/2}},$$

we run into the problem of how to effectively parametrize number fields. This problem is avoided in the present paper by choosing a special class of number fields: Let l be a fixed rational prime and

$$S_l := \{m \in \mathbb{N} \setminus \{1\} \,|\, m \text{ is } l\text{–power–free}\}.$$

For $m \in S_l$, define the pure number field $k_m := \mathbb{Q}(\sqrt[l]{m})$ where the radical is choosen in $\mathbb{R}^+$. Let $r(m) := \operatorname{res}_{s=1} \zeta_{k_m}(s)$ where ζ_{k_m} is the Dedekind zeta function of k_m. Then

$$r(m) = \frac{h_{k_m} R_{k_m}}{d_{k_m}^{1/2}} c(l), \quad c(l) = \left\{ \begin{array}{ll} 2, & l = 2, \\ (2\pi)^{(l-1)/2}, & l \geq 3, \end{array} \right\}$$

and $d_{k_m} \asymp K(m)^{l-1}$, where $K(m)$ is the squarefree kernel of m. For $m \in \mathbb{N} \setminus S_l$, define $r(m) := 0$.

Theorem. *There is a distribution function $F \in C^\infty(\mathbb{R})$ such that for all $z \in \mathbb{R}$,*

$$\lim_{x\to\infty} \frac{\#\{m \in S_l \,|\, m \leq x,\, r(m) \leq e^z\}}{\#\{m \in S_l \,|\, m \leq x\}} = F(z).$$

Furthermore,

$$\lim_{x\to\infty} \frac{1}{\#\{m \in S_l \,|\, m \leq x\}} \sum_{m \in S_l : m \leq x} r(m)^q = \int_{\mathbb{R}^+} z^q \, dF(\log z)$$

for all $q \in \mathbb{N}$. The characteristic function $\Psi(t)$ of F is an Euler product whose factors depend on $t \in \mathbb{R}$.

In order to give an idea of the proof let us first review the method for the well-known case $l = 2$. For $m > 1$ squarefree, Dirichlet's class number formula gives

$$\zeta_{\mathbb{Q}(\sqrt{m})}(s) = \zeta(s)\, L(s, \chi_d),$$

where

$$d = \left\{ \begin{array}{ll} m, & m \equiv 1 \bmod 4, \\ 4m, & m \equiv 2, 3 \bmod 4, \end{array} \right\}$$

is the discriminant of $\mathbb{Q}(\sqrt{m})$ and χ_d is the Jacobi character for the modulus $|d|$. Therefore

$$r(m) = L(1, \chi_d) = \sum_{n\geq 1} \frac{\chi_d(n)}{n} = \prod_p \left(1 - \frac{\chi_d(p)}{p^s}\right)^{-1}\Big|_{s=1}.$$

The idea of proof is as follows: For $q \geq 1$, the function r is approximated in the q–th mean by functions R_P, $P \in \mathbb{N}$, such that

$$\|r - R_P\|_q \to 0 \text{ as } P \to \infty. \tag{1}$$

Here

$$\|f\|_q := \Big(\limsup_{x\to\infty} \frac{1}{x} \sum_{m\le x} |f(m)|^q\Big)^{1/q} \in [0,\infty]$$

for $f : \mathbb{N} \to \mathbb{C}$. The functions R_P are partial products of the Euler product above, i.e.

$$R_P(m) := \prod_{p\le P} \Big(1 - \frac{\chi_d(p)}{p}\Big)^{-1}.$$

They are periodic in m since for $p > 2$, we have

$$\chi_d(p) = \Big(\frac{d}{p}\Big) = \left\{\begin{array}{ll} 1, & x^2 \equiv d \bmod p \text{ solvable}, p \not| d, \\ -1, & x^2 \equiv d \bmod p \text{ unsolvable}, \\ 0 & p|d. \end{array}\right\}$$

Since periodic functions have limit distributions a standard procedure shows the same for r. In fact the procedure in this last step is somewhat different since we also want to show the smoothness of F.

The approximation (1) could be done with character sum estimates. More suitable for generalizations is the following method which uses contour integration and zero density estimates. Let $\mathcal{K}$ be the rectangle with vertices $2+iT$, $\gamma+iT$, $\gamma-iT$ and $2-iT$, and $N, T \ge 1$ and $1/2 < \gamma < 1$ free parameters. The Residue Theorem gives

$$\frac{1}{2\pi i}\int_{\mathcal{K}} L(s,\chi_d)\,\Gamma(s-1)\,N^{s-1}ds = L(1,\chi_d).$$

Since the Γ-function decays exponentially in vertical strips of finite width the limit $T \to \infty$ together with Mellin's inversion formula gives

$$L(1,\chi_d) = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} - \frac{1}{2\pi i}\int_{\gamma-i\infty}^{\gamma+i\infty} = \sum_{n\ge1} \frac{\chi_d(n)}{n} e^{-n/N} - I(m,N).$$

If we assume the Generalized Lindelöf Hypothesis

$$L(s,\chi_d) \ll_\epsilon (d(1+|\Im s|))^\epsilon \tag{2}$$

for $\gamma \le \Re s \le 1$ and $m > 1$ squarefree, we easily get the estimate

$$I(m,N) \ll_\epsilon d^\epsilon N^{\gamma-1}. \tag{3}$$

Here it is important that the exponent of d can be made arbitrarily small and the exponent of N is negative.

Without any assumption this procedure can be immitated as follows: If $L(s,\chi_d)$ has no zeros in the rectangle

$$\{s \in \mathbb{C} \,|\, \Re s \ge \gamma - \epsilon,\ |\Im s| \le (\log x)^2\}, \tag{4}$$

then the usual combination of the Borel-Carathéodory Theorem and Hadamard's Three Circles Theorem gives (2) for $\gamma \le \Re s \le 2$ and $|\Im s| \le (\log x)^2/2$. Using the exponential decay of the Γ-function on $|\Im s| \ge (\log x)^2/2$ we again get (3). If there is a zero of $L(s,\chi_d)$ in the rectangle (4) all we can say is that

$$I(m,N) \ll d^\epsilon + N^\epsilon.$$

Now zero density estimates can be used to show that the second case does not happen too often, i.e.

$$\#\{1 < m \le x \mid m \text{ squarefree}, L(s,\chi_d) \text{ has a zero in the rectangle (4)}\} \ll_\epsilon x^{1-c(\gamma)+\epsilon}$$

with some constant $c(\gamma) > 0$.

In the q–th mean we have the approximation

$$\sum_{n\ge 1} \frac{\chi_d(n)}{n} e^{-n/N} \approx \sum_{n\le N} \frac{\chi_d(n)}{n}.$$

Choosing N as a small power of x proves the statement (1).

In the general case $l \ge 2$ we have, for $\Re s > 1$,

$$\begin{aligned}\zeta_{k_m}(s) &= \prod_p \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{p^{f(\mathfrak{p}/p)s}}\right)^{-1} \\ &= \prod_p \prod_{\mathfrak{p}|p:\, f(\mathfrak{p}/p)\ge 2} \left(1 - \frac{1}{p^{f(\mathfrak{p}/p)s}}\right)^{-1} \prod_p \left(1 - \frac{1}{p^s}\right)^{-\chi(m,p)} \zeta(s),\end{aligned}$$

where $f(\mathfrak{p}/p) := [\mathcal{O}_{k_m}/\mathfrak{p} : \mathbb{Z}/p\mathbb{Z}]$ is the residue class degree of $\mathfrak{p}$ and

$$\chi(m,p) := \#\{\mathfrak{p}|p \mid f(\mathfrak{p}/p) = 1\} - 1.$$

Thus

$$r(m) = \prod_p \prod_{\mathfrak{p}|p:\, f(\mathfrak{p}/p)\ge 2} \left(1 - \frac{1}{p^{f(\mathfrak{p}/p)}}\right)^{-1} \left(1 - \frac{1}{l}\right)^{-\chi(m,l)} \prod_{p\ne l} \left(1 - \frac{1}{p^s}\right)^{-\chi(m,p)} \Bigg|_{s=1}.$$

In order to get the almost periodicity of the partial products of this Euler product we exploit the relation between the splitting of rational primes p in k_m and the splitting of $X^l - m$ in $\mathbb{F}_p[X]$ and $\mathbb{Q}_p^{\text{unram}}[X]$. Here $\mathbb{Q}_p^{\text{unram}}$ is the maximal unramified extension of $\mathbb{Q}_p$. The following lemmas give the necessary information.

Lemma. *For $p \ne l$, we have*

$$\chi(m,p) = \#\{x \bmod p \mid x^l \equiv m \bmod p\} - 1.$$

In particular, the function $\chi(\cdot, p)$ is p–periodic and

$$\sum_{m \bmod p} \chi(m,p) = 0,$$

which serves as a substitute for the orthogonality relation for characters.

Lemma. *Let p be a prime, $m \in S_l$ and $b \in \mathbb{N}_0$ such that $p^b \| m$. Then the factor*

$$\prod_{\mathfrak{p}|p:\, f(\mathfrak{p}/p)\ge 2} \left(1 - \frac{1}{p^{f(\mathfrak{p}/p)}}\right)^{-1}$$

is constant on the residue class $m \bmod p^{b(l-1)+l\,\mathrm{ord}_p l+1}$.

Both lemmas are used to show the almost periodicity of R_P in the general case. In order to prove the approximation (1) we use the following zero density estimate of Kawada [7].

Theorem. *For sufficiently small $\eta > 0$, we have*

$$\sum_{m \in S_l : x < m \le 2x} N(m; 1-\eta, T) \ll (xT)^{1-\eta}, \quad x \ge T \ge 1,$$

where $N(\ldots)$ is the number of zeros of $\zeta_{k_m}(s)\zeta(s)^{-1}$ in the rectangle $[1-\eta, 1] \times [-T, T]$.

References

[1] M.B. Barban, The "Large Sieve" method and its applications in the theory of numbers, Russian Math. Surveys 2(1966), 49–103

[2] F. Chamizo, H. Iwaniec, On the Gauß mean value formula for class numbers, Nagoya Math. J. 151(1998), 199–208

[3] S. Chowla, P. Erdös, A theorem on the distribution of values of L–series, J. Indian Math. Soc. 15(1951), 11–18

[4] P.D.T.A. Elliott, On the distribution of the values of quadratic L–series in the half–plane $\sigma > 1/2$, Invent. math. 21(1973), 319–338

[5] C.F. Gauss, Disquisitiones Arithmeticae, Leipzig 1801

[6] M. Jutila, On character sums and class numbers, J. Number Th. 5(1973), 203–214

[7] K. Kawada, A zero density estimate for Dedekind zeta functions of pure extension fields, Tsukuba J. Math. 22(1998), 357–369

[8] S. Lang, Algebraic Number Theory, Graduate Texts in Mathematics 110, Springer, New York 1994

[9] F. Mertens, Über einige asymptotische Gesetze der Zahlentheorie, J. Reine Angew. Math. 77(1874), 289–338

[10] T. Shintani, On zeta–functions associated with the vector space of quadratic forms, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 22(1975), 25–65

[11] C.L. Siegel, The average measure of quadratic forms with given determinant and signature, Ann. of Math. 45(1944), 667–685

[12] I.M. Vinogradov, On the number of integer points in a sphere, Izv. Akad. Nauk SSSR, Ser. Mat. 27(1963), 957–968

[13] D. Wolke, Moments of class numbers III, J. Number Th. 4(1972), 523–531

Mathematisches Institut, Albert-Ludwigs-Universität, Eckerstr. 1, D-79104 Freiburg
E-mail address: manfred.peter@math.uni-freiburg.de